

**AMENDMENT TO RULES COMM. PRINT 119–8**  
**OFFERED BY MR. GARBARINO OF NEW YORK**

Add at the end of subtitle A of title XVII of division  
A the following:

**1 SECTION 1. SHORT TITLE.**

2       This Act may be cited as the “Widespread Informa-  
3 tion Management for the Welfare of Infrastructure and  
4 Government Act”.

**5 SEC. 2. REAUTHORIZATION OF THE CYBERSECURITY ACT**  
**6 OF 2015.**

7       (a) IN GENERAL.—The Cybersecurity Act of 2015 (6  
8 U.S.C. 1501 et seq.; enacted as division N of the Consoli-  
9 dated Appropriations Act, 2016; Public Law 114–113) is  
10 amended—

11           (1) in section 102 (6 U.S.C. 1501; relating to  
12 definitions)—

13                   (A) by redesignating paragraphs (4), (5),  
14                   (6), (7), (8), (9), (10), (11), (12), (13), (14),  
15                   (15), (16), (17), and (18) as paragraphs (6),  
16                   (7), (8), (9), (10), (11), (12), (13), (14), (15),  
17                   (16), (17), (18), (19), and (20), respectively;  
18                   and

1 (B) by inserting after paragraph (3) the  
2 following new paragraphs:

3 “(4) ARTIFICIAL INTELLIGENCE.—The term  
4 ‘artificial intelligence’ has the meaning given such  
5 term in section 5002 of the National Artificial Intel-  
6 ligence Initiative Act of 2020 (15 U.S.C. 9401).

7 “(5) CRITICAL INFRASTRUCTURE.—The term  
8 ‘critical infrastructure’ has the meaning given such  
9 term in section 1016(e) of Public Law 107–56 (42  
10 U.S.C. 5195c(e)).”;

11 (2) in section 103 (6 U.S.C. 1502; relating to  
12 sharing of information by the Federal Govern-  
13 ment)—

14 (A) in subsection (a), in the matter pre-  
15 ceding paragraph (1), by striking “develop and  
16 issue” and inserting “develop, issue, and, as ap-  
17 propriate, update”; and

18 (B) in subsection (b)—

19 (i) in paragraph (1)—

20 (I) in the matter preceding sub-  
21 paragraph (A), by inserting “and, as  
22 appropriate, updated,” after “devel-  
23 oped”;

24 (II) by amending subparagraph  
25 (A) to read as follows:

1           “(A) ensure the Federal Government has  
2           and maintains the capability to share cyber  
3           threat indicators and defensive measures in  
4           real-time consistent with the protection of clas-  
5           sified information, and maintains the capability  
6           to provide technical assistance, on a voluntary  
7           basis, to non-Federal entities in utilizing cyber  
8           threat indicators and defensive measures for cy-  
9           bersecurity purposes;”;

10                       (III) in subparagraph (E)(ii), by  
11                       striking “and” after the semicolon;

12                       (IV) in subparagraph (F), by  
13                       striking the period and inserting “;  
14                       and”; and

15                       (V) by adding at the end the fol-  
16                       lowing new subparagraph:

17           “(G) pursuant to section 2212 of the  
18           Homeland Security Act of 2002 (6 U.S.C. 662),  
19           provide one-time read-ins, as appropriate, to se-  
20           lect individuals identified by non-Federal enti-  
21           ties that own or operate critical infrastructure  
22           or artificial intelligence;”;

23                       (ii) in paragraph (2)—

1 (I) by inserting “and, as appro-  
2 priate, updating,” after “developing”;  
3 and

4 (II) by inserting “and defensive  
5 measures” after “promote the sharing  
6 of cyber threat indicators”; and

7 (C) in subsection (c)—

8 (i) by inserting “and not later than 60  
9 days after any update, as appropriate, of  
10 procedures required by subsection (a),”  
11 after “Act,”; and

12 (ii) by inserting “(or update, as ap-  
13 propriate)” after “procedures”;

14 (3) in section 104 (6 U.S.C. 1503; relating to  
15 authorizations for preventing, detecting, analyzing,  
16 and mitigating cybersecurity threats)—

17 (A) in paragraph (3) of subsection (c)—

18 (i) in the matter preceding subpara-  
19 graph (A), by striking “shall be” and in-  
20 serting “may be”;

21 (ii) in subparagraph (A), by striking  
22 “or” after the semicolon;

23 (iii) in subparagraph (B), by striking  
24 the period and inserting “; or”; and

1 (iv) by adding at the end the following  
2 new subparagraph:

3 “(C) to preclude the use of artificial intel-  
4 ligence that is strictly deployed for cybersecu-  
5 rity purposes in carrying out the activities au-  
6 thorized under paragraph (1) provided that  
7 such deployment complies with section  
8 105(d)(5).”; and

9 (B) in subparagraph (B) of subsection  
10 (d)(2), by inserting “, which may utilize artifi-  
11 cial intelligence that is strictly deployed for cy-  
12 bersecurity purposes,” after “technical capa-  
13 bility”;

14 (4) in section 105 (6 U.S.C. 1504); relating to  
15 sharing of cyber threat indicators and defensive  
16 measures with the Federal Government)—

17 (A) in subsection (a)—

18 (i) in paragraph (2), by adding at the  
19 end the following new sentences: “As ap-  
20 propriate, the Attorney General and the  
21 Secretary of Homeland Security shall, in  
22 consultation with the heads of the appro-  
23 priate Federal entities, jointly update such  
24 policies and procedures, and issue and  
25 make publicly available such updated poli-

1           cies and procedures. Such updates shall  
2           prioritize rapid dissemination to State,  
3           local, Tribal, and territorial governments  
4           and owners and operators of non-Federal  
5           critical infrastructure or artificial intel-  
6           ligence of relevant and actionable cyber  
7           threat indicators and defensive measures.”;

8           (ii) in paragraph (3), in the matter  
9           preceding subparagraph (A), by striking  
10          “developed or issued” and inserting “devel-  
11          oped, issued, or, as appropriate, updated,”;  
12          and

13          (iii) in paragraph (4)—

14               (I) in subparagraph (A), by add-  
15               ing at the end the following new sen-  
16               tence: “As appropriate, the Attorney  
17               General and the Secretary of Home-  
18               land Security shall jointly update and  
19               make publicly available such guidance  
20               to so assist entities and promote such  
21               sharing of cyber threat indicators and  
22               defensive measures with such Federal  
23               entities under this title.”; and

24               (II) in subparagraph (B), in the  
25               matter preceding clause (i), by insert-

1 ing “and, as appropriate, updated,”  
2 after “developed”;

3 (B) in subsection (b)—

4 (i) in paragraph (2)(B), by inserting  
5 “, and, as appropriate, update,” after “re-  
6 view”; and

7 (ii) in paragraph (3), in the matter  
8 preceding subparagraph (A), by inserting  
9 “and, as appropriate, updated,” after “re-  
10 quired”; and

11 (C) in subsection (c)—

12 (i) in paragraph (1)(D), by inserting  
13 “, including if such capability and process  
14 employs artificial intelligence” before the  
15 semicolon; and

16 (ii) in paragraph (2), by adding at the  
17 end the following new subparagraph:

18 “(C) OUTREACH.—Not later than 90 days  
19 after the date of the enactment of this subpara-  
20 graph, the Secretary of Homeland Security  
21 shall develop and continuously implement an  
22 outreach plan, including targeted engagement,  
23 to ensure Federal and non-Federal entities,  
24 particularly small or rural owners or operators  
25 of critical infrastructure which often lack dedi-

1 cated cybersecurity staff but remain vital to na-  
2 tional security—

3 “(i) are aware of the capability and  
4 process required by paragraph (1) to share  
5 cyber threat indicators and defensive meas-  
6 ures, including the benefits real-time infor-  
7 mation sharing provides;

8 “(ii) understand how to share cyber  
9 threat indicators and defensive measures;

10 “(iii) understand the obligation to re-  
11 move certain personal information in ac-  
12 cordance with section 104(d)(7) prior to  
13 sharing a cyber threat indicator;

14 “(iv) understand how cyber threat in-  
15 dicators and defensive measures are re-  
16 ceived, processed, used, and protected;

17 “(v) understand the protections they  
18 are afforded in sharing any cyber threat  
19 indicators and defensive measures; and

20 “(vi) can provide feedback to the Sec-  
21 retary when policies, procedures, and  
22 guidelines that are unclear or unintention-  
23 ally prohibitive to sharing cyber threat in-  
24 dicators and defensive measures.”; and



1 (iii) by adding at the end the fol-  
2 lowing new subparagraph:

3 “(D) BRIEFINGS ON OUTREACH.—The  
4 Secretary of Homeland Security shall annually  
5 provide to the Committee on Homeland Secu-  
6 rity of the House of Representatives and the  
7 Committee on Homeland Security and Govern-  
8 mental Affairs of the Senate a briefing on the  
9 implementation of outreach pursuant to sub-  
10 paragraph (B).”; and

11 (D) in subsection (d)—

12 (i) in paragraph (1), by inserting  
13 “copyright or” before “trade secret protec-  
14 tion”; and

15 (ii) in paragraph (5)(A),

16 (I) in clause (iv), by striking  
17 “or” after the semicolon;

18 (II) in clause (v)(III), by striking  
19 the period and inserting “; or”; and

20 (III) by adding at the end the  
21 following new clause:

22 “(vi) the purpose of rapidly providing  
23 to other Federal entities awareness of a cy-  
24 bersecurity threat that may impact the in-  
25 formation systems of such Agencies.”;

1           (5) in section 108 (6 U.S.C. 1507; relating to  
2       construction and preemption)—

3           (A) in subsection (c)—

4               (i) in the matter preceding paragraph  
5               (1), by striking “shall be” and inserting  
6               “may be”;

7               (ii) in paragraph (2), by striking “or”  
8               after the semicolon;

9               (iii) in paragraph (3), by striking the  
10              period and inserting “; or”; and

11              (iv) by adding at the end the following  
12              new paragraph:

13              “(4) to preclude the use of artificial intelligence  
14              that is strictly deployed for cybersecurity purposes in  
15              carrying out activities authorized by this title.”; and

16           (B) in subsection (f)(3)—

17               (i) by inserting “to share cyber threat  
18               indicators or defensive measures” after  
19               “relationship”; and

20               (ii) by striking “or” after the semi-  
21               colon;

22           (6) in section 109 (6 U.S.C. 1508; relating to  
23       report on cybersecurity threats)—

24           (A) in subsection (a)—

1 (i) by inserting “and not later than  
2 September 30 of every two years there-  
3 after,” after “Act,”;

4 (ii) by inserting “the Secretary of  
5 Homeland Security and” after “in coordi-  
6 nation with”;

7 (iii) by inserting “and the Committee  
8 on Homeland Security and Governmental  
9 Affairs” before “of the Senate”;

10 (iv) by inserting “and the Committee  
11 on Homeland Security” before “of the  
12 House”; and

13 (v) by inserting “prepositioning activi-  
14 ties, ransomware,” after “attacks,”; and  
15 (B) in subsection (b)—

16 (i) in paragraph (1), by inserting  
17 “prepositioning activities, ransomware,”  
18 after “attacks,”;

19 (i) in paragraph (2), by inserting  
20 “prepositioning activity, ransomware,”  
21 after “attack,”;

22 (i) in paragraph (3), by inserting  
23 “prepositioning activities, ransomware,”  
24 after “attacks,” each place it appears; and

1 (i) in paragraph (4), by inserting  
2 “prepositioning activities, ransomware,”  
3 after “attacks,”; and

4 (7) in section 111(a) (6 U.S.C. 1510(a), relat-  
5 ing to effective period), by striking “2025” and in-  
6 serting “2035”.

7 (b) CONFORMING AMENDMENTS.—Section 2200 of  
8 the Homeland Security Act of 2002 (6 U.S.C. 650; relat-  
9 ing to definitions) is amended—

10 (1) in paragraph (5)—

11 (A) in subparagraph (B), by inserting “or  
12 compromising” after “defeating”;

13 (B) in subparagraph (C), by inserting “in-  
14 cluding a security vulnerability affecting an in-  
15 formation system or a technology included in  
16 the critical and emerging technologies list of the  
17 Office of Science and Technology Policy or suc-  
18 cessor list, such as artificial intelligence (as  
19 such term is defined in section 5002 of the Na-  
20 tional Artificial Intelligence Initiative Act of  
21 2020 (15 U.S.C. 9401)), which may be in a  
22 Federal entity’s or non-Federal entity’s soft-  
23 ware or hardware supply chain,” after “security  
24 vulnerability,”;

1 (C) in subparagraph (D), by inserting “or  
2 compromise” after “defeat”; and

3 (D) in subparagraph (F), by inserting “or  
4 compromised” after “exfiltrated”;

5 (2) in paragraph (14), by amending subpara-  
6 graph (B) to read as follows:

7 “(B) includes, in accordance with section  
8 104(d)(2) of the Cybersecurity Sharing Act of  
9 2015 (6 U.S.C. 1503(d)(2)), operational tech-  
10 nology, including industrial control systems,  
11 such as supervisory control and data acquisition  
12 systems, distributed control systems, and pro-  
13 grammable logic controllers.”; and

14 (3) in paragraph (25), by inserting “or com-  
15 promise” after “defeat”.

